FIGHTING FRAUD

Digital Fraud Is Changing. Are You Ready?

Is your digital transformation ready for the latest cyber-criminal tactics? For over a decade, Kount has been deploying the latest technology and proven processes to detect and deter fraud, protecting organizations around the world. As fraud attacks increase in frequency and sophistication, companies operating in online and mobile channels are at ever-increasing risk. Let Kount show you why enterprises rely on our expertise to protect their topline and bottom line. **Contact Kount today.**

fraudfighter@kount.com

Certainty in Every Digital Interaction ❯ kount.com

Kount®

FIGHTING FRAUD

Distributed in
THE TIMES

raconteur reports

Publishing manager
Hannah Smallman

Production editor
Benjamin Chiou

Managing editor
Peter Archer

Head of production
Justyna O'Connell

Digital content executive
Fran Cassidy

Design
Grant Chapman
Sara Gelfgren
Kellie Jerrard
Harry Lewis-Irlam
Samuele Motta

Head of design
Tim Whitlock

Smart machines snare fraudsters

Artificial intelligence and machine-learning are fast becoming essential weapons in the war on fraud

OLIVER PICKUP


isak55/Shutterstock

The phrase "loose lips might sink ships" warned, on American wartime posters, of unguarded conversations during the Second World War. Now, 73 years on from Victory over Japan Day on September 2, 1945, the formal conclusion of that horrific epoch, a similarly sloppy attitude to cybersecurity in the workplace can torpedo organisations.

A well-cast "phish" – a fraudulent attempt to hook sensitive data such as usernames, passwords and codes – is capable of inflicting fatal financial and repetitional damage. "Successful phishing attacks can sink companies as well as individuals," says Juliette Rizkallah, chief marketing officer at identity software organisation SailPoint, updating the famous idiom.

Fraud is endemic in the digital age. The UK loses over £190 billion per year to fraud – more than the government spends on health and defence – according to credit service agency Experian. Organisations of all sizes are failing to keep pace with threats, mostly because of poor human cyber-hygiene. Little wonder hordes of business leaders are turning to artificial intelligence (AI) to fight fraud.

So how can autonomous technology help? "Artificial intelligence is befitting fighting fraud because it picks up on patterns and irregularities that humans can't naturally perceive," says Stuart Aston, national security officer of Microsoft UK. He points out his organisation's Azure Machine Learning is enabling Callcredit, one of the UK's largest credit reference agencies, to identify criminals who pretend to be someone else when trying to access credit reports and borrow money.

"There are a number of promising innovations, including the ability to look at rich data previously excluded from fraud detection, such as photographs, video and translated audio, that are revolutionising fraud prevention, and with AI tools these tasks can be conducted faster, more efficiently and more precisely than before," says Mr Aston.

A growing cluster of similar AI-powered fraud prevention software applications are now on the market, such as iovation, pipl and Zonos, though criminals are using the same capabilities in nefarious ways.

"Machine-learning will be essential in developing faster, more intuitive AI, but the flip side to that is hackers can deploy machine-learning too," says Richard Lush, head of cyber-operational security at CGI UK. "An example of this is Deeplocker, which can use AI to hide malware. That's why it's really important to dovetail technology with human operators who can bring a level of empathy and intuition that AI currently cannot."

Luke Vile, cybersecurity operations director at 2-sec, concurs that adopting AI to combat fraudulent attacks is becoming essential. "AI can help to flag fraudulent activity extremely quickly, often within seconds, so that possible crime can be stopped or spotted immediately," he says. "AI can also be tuned to only alert organisations to fraud rather than 'possible fraud', meaning security teams are not spending too much time on activity that is safe, but unusual."

Martin Balek, machine-learning research director at internet security giant Avast, expands this theme. "AI hasn't just improved defences, it has remodelled security with its ability to detect threats in real time and accurately predict emerging threats," he says. "This is a giant leap forward for the industry. Before AI, this sort of task would require monumental resource for humans to perform alone."

While it is likely that before long we will reach the point where a fully automated, AI-based security system will be effective enough to eliminate a high percentage of fraud without requiring any human input – indeed, Feedzai recently announced it is bringing automated learning to the fraud space, claiming this to be an industry first – many within advise that sign-off is not handed solely to a machine.

"Organisations will always want a final, human pair of eyes to make sure that obvious errors aren't being caused," says Mr Vile.

And Mr Lush notes: "Google Cloud are bringing more humans on board to work in their fraud detection operations to safeguard their related customer service offer, so it's too early to tell if fraud prevention will be fully automated, resulting in the total of exclusion of humans."

Mr Balek adds: "Full automation also has implications under the general data protection regulation (GDPR). Bearing in mind that such technology could constrain the ability of consumers to use their own funds, or to achieve desired outcomes, a company seeking to implement full AI would need to display a high level of transparency about its operations.

"Article 13 of the GDPR is clear that the existence of automated decision-making, meaningful information about the logic involved, and the significance and envisaged consequences of such processing, must be published to individuals whose personal data is to be subjected to this processing."

Limor Kessem, executive security adviser at IBM Security, believes multi-verification points, plus the introduction of effective biometric authentication, again using AI, and removing memorable passwords altogether will bolster digital defences.

"Consumer attitudes and preferences will lead the way in reducing password use and layering security controls to put more hurdles in an attacker's way," she says. "On its own, there is not one method that could be considered 'unhackable', but layering more than one element can definitely turn hacking an account into a costly endeavour for a criminal.

"In the longer term, AI is sure to become a key part of the way organisations prevent fraud. We need to change the way we manage fraud and face attackers with adaptive technologies that reason like humans do. Over time, these technologies will likely keep reducing fraud rates until a breaking point where the criminal's return on investment will no longer be lucrative enough." ◆

49%

of global organisations say they have been a victim of fraud and economic crime within the last 24 months

PwC 2018

22%

say they are using and deriving value from pattern-recognition technologies in combating fraud

11%

are using and deriving value from artificial intelligence

THERANOS

Jason Doiy/Getty Images

01

Bad blood is being shed in Silicon Valley

With billions at stake, along with pride and reputation, business leaders must avoid the trap of making fraudulent claims

SHARON THIRUCHELVAM

Few companies seem to encapsulate the worst excesses of Silicon Valley better than Theranos. The supposedly revolutionary blood-testing startup achieved a valuation of $9 billion, only to face allegations of hype and lies.

John Carreyrou, a journalist at *The Wall Street Journal,* broke the story in 2015, just as Theranos's product was on the cusp of being rolled out in 8,000 Walgreen pharmacy stores. His book, *Bad Blood: Secrets and Lies in a Silicon Valley Startup*, documents just how an alleged deception was nearly pulled off.

A morality tale for our times, the Theranos saga centres on Elizabeth Holmes, a serious and driven young woman who dropped out of Stanford University in 2003 to found the company when she was just 19 years old.

"Elizabeth Holmes did not set out to pull a long con," says Mr Carreyrou. "She really did think her vision for this product would do good for society – that it would revolutionise blood testing and help medicine."

With no medical training, Ms Holmes sought with her team to score an audacious hat trick that had eluded medical scientists for decades: to take diagnostic blood tests from a finger prick, rather than intravenous needle; to combine multiple blood tests from vitamin deficiency, to disease and pregnancy tests in one diagnostic tool; and to miniaturise testing equipment into a portable device without compromising accuracy.

The product would be low cost and available to use in every home in America. The power of such a thing was plain to see. It would revolutionise healthcare. "I believe the individual is the answer to the challenges of healthcare, but we can't engage the individual in changing outcomes unless individuals have access to the information they need," Ms Holmes said in her 2014 TED Talk.

She yearned for success. "She wanted to join the pantheon of tech startup billionaires and be the first woman to do so," says Mr Carreyrou.

Her only problem was that Theranos was allegedly nowhere near achieving her stated goals when its product was brought to market.

Ms Holmes stands accused of making the fundamental and unforgivable error of applying Silicon Valley's "fake it until you make it" mindset to medical care, Mr Carreyrou claims. Releasing a "buggy" app in beta stage is one thing. "But she was trying to build a medical product upon which doctors and patients make very important decisions – some of them life and death," he says.

Some 70 per cent of doctors' decisions are based on blood test results; a faulty Theranos product would endanger lives, a fact that Ms Holmes seemed to fail to see.

At the same time, her single-minded drive, self-belief and brilliant sales pitch won her champions in high places. A Palo Alto native, family connections introduced her to the Oracle billionaire Larry Ellison and the venture capital hero Tim Draper. The Theranos board became peopled with military generals, such as John "Mad Dog" Mattis, now secretary of defence in the Trump administration, and former secretaries of state George Shultz and Henry Kissinger.

"She wows all these guys with larger-than-life reputations with her vision; she convinces them to join her board and they increase her credibility," says Mr Carreyrou.

Ms Holmes had a unique ability to win people's confidence. She idolised Steve Jobs to the extent that she adopted a daily uniform of black rollnecks and affected a deep baritone voice, speaking several octaves beneath her natural register. These curious qualities, combined with her charm, intelligence and large, blue and unblinking eyes created the aura of someone exceptional.

"There is a myth in Silicon Valley around founders," says Mr Carreyrou, "The greatest culprit of which is Steve Jobs. He has been turned into such an icon and hero of American capitalism that it has created the myth of the startup founder who can see around corners and do no wrong. It has created this culture of incredible entitlement and magical thinking among startup founders in the Valley."

It is claimed that Ms Holmes' vaulting ambition and idealism were poisoned by hubris. The corporate culture she and Theranos's president Sunny Balwani fostered was allegedly dysfunctional to the point of dehumanising. Allegedly founded on fear, paranoia, secrecy and bullying, teams were siloed and pitted against each other. Unquestioning loyalty was demanded from employees and dissent, however well intentioned, was punished with dismissal, it is claimed.

She took control of all decision-making. The board could not achieve quorum without her and the company used non-disclosure agreements to silence former employees. A culture of secrecy seemingly enabled a small inner circle allegedly to mislead and deceive Theranos staff, its board, investors, commercial partners, clients, members of the press and even federal regulators the Food and Drug Administration, and the Centers for Medicare and Medicaid Services.

When challenged, the lengths Ms Holmes and Mr Balwani allegedly scaled to protect the company stretch the limits of credulity. It is claimed they surveilled, blackmailed, intimidated and litigated against critics, enemies and competitors. When Mr Carreyrou's investigations neared publication, Ms Holmes allegedly leaned on Rupert Murdoch, who was a late investor in Theranos and whose News Corporation group owns *The Wall Street Journal*, to kill the story.

> **Steve Jobs has been turned into such an icon and hero of American capitalism that it has created the myth of the startup founder who can see around corners and do no wrong**

Now indicted for criminal fraud, Ms Holmes is said to have cast herself as a victim. "She feels as if she is a startup founder who ended up failing and because she is a woman the press has piled in on her," says Mr Carreyrou. "She has this Joan of Arc syndrome. She feels like a martyr."

The question remains whether Silicon Valley will learn from her experience and question the uncritical adulation of startup founders. "I certainly believe there has been an evolution in the way the American press covers Silicon Valley, but I am not sure people's values in the Silicon Valley echo chamber have changed," says Mr Carreyrou. "Time will tell." ◆


Michael Lionstar

02

David Paul Morris/Bloomberg via Getty Images

03

01 Theranos headquarters, Palo Alto, California

02 Journalist John Carreyrou

03 Theranos founder and chief executive Elizabeth Holmes

Commercial feature

Countering the threat from within

As the battle against insider fraud continues to intensify, the need for intelligent technology to counter the threat looks set to keep growing

Fraud committed by insiders is a large and growing threat to companies. Systems that monitor abnormal behaviour have become a major weapon in the fight against the threat of insider fraud. But many companies are behind the curve in adopting such systems.

Here are two examples of how "behaviour intelligence" technologies are saving companies millions from the insider threat.

A US bank found that a new employee had been typing questions into Google frequently about how to do their job, much more so than any of their peers. The company's security system flashed a warning signal about this abnormal behaviour. It was revealed that the employee was a fraudster who had fabricated their experience to get the job so they could access the company's data.

Another bank employee was found to have been creating unusual spreadsheets with data taken from business systems, again through a warning signal about abnormal behaviour from its security system. By checking the data against the company's financial statistics, the bank discovered they and another individual with privileged access were insider dealing.

Mark Coates
Vice president, EMEA

Organisations that fall victim to fraud on average see their share price fall 5 per cent on the day a breach is disclosed, according to the Ponemon Institute. Falls range from 3 per cent for companies with good security to 7 per cent for companies with poor security. The average cost to organisations is $8.7 million (£6.8 million) per incident.

One of the biggest problems companies face in protecting against fraud is the insider threat; 60 per cent of all attacks are carried out by insiders, according to IBM. The Dtex *2018 Insider Threat Intelligence Report* revealed that 100 per cent of all organisations assessed have active insider threats in play.

To make matters worse, 76 per cent of insider incidents are not prosecuted, due to lack of evidence.

Many companies in banking and other industries are failing to detect or prosecute insider frauds because their security systems lack visibility on suspicious activity. There are thousands of abnormal behaviours that may indicate a potential fraud. Behaviour intelligence technology is effective because it can provide an early-warning signal for prevention and forensic evidence if an act is committed.

The insider threat is often from privileged users, who are employees, contractors or partners with access to almost every corner of the corporate network. These individuals do not need to use sophisticated hacking software. They can often execute a fraud with existing software that is familiar to them.

> **Enabling early visibility, with a fast signal into abnormal behaviour can help to eliminate or reduce that insider threat**

The General Data Protection Regulation (GDPR), which came into force this year, could have unintentionally made this situation worse by making it more attractive to criminals to plant or bribe an insider to misappropriate data, with privileged users being primary targets.

GDPR mandates heavy fines for companies that suffer a data breach. Penalties can reach up to 4 per cent of a violators' annual revenue, which in many cases will far outweigh the actual cost of a breach.

Rather than sell stolen data to fellow criminals or exact a ransom to unencrypt it for smaller amounts, criminals will extort money from organisations for not exposing data thefts publicly, which would trigger fines.

The ransom will be much higher than any sum the criminals could have previously made through black market sales or ransomware decryption, but significantly lower than a GDPR fine. This could prompt companies to pay extortion rather than face high penalties. Malicious privileged users may be all too willing to take a bribe, especially when they know that their organisations have no visibility into what they are doing and that a massive pay day would never be revealed publicly.

Mark Coates, Europe, Middle East and Africa (EMEA) vice president, and Ben Kennedy, UK and South Africa sales director at Dtex Systems, say that despite these increasing dangers, most companies do not have stringent systems for spotting insider threats.

"Maliciously fraudulent activity is increasing," says Mr Coates. "Most organisations focus on monitoring movers, joiners and leavers. But there is a real insider threat from privileged users, who have the 'keys to the kingdom' and are savvy about not being spotted. If these individuals are open to bribery, the rewards can be huge.

"Enabling early visibility, with a fast signal into abnormal behaviour, can help to eliminate or reduce that insider threat. Dtex has a library of thousands of patterns of abnormal behaviour, scored according to potential threat level. We have built that database over 12 years to create a high-fidelity signal that minimises the number of false alerts.

"To be credible in this field, you need deep experience in understanding these behaviours, so you can benchmark them quickly. We have a wealth of knowledge and already know what 'bad' looks like, from monitoring against peer groups, within and across industries."

Mr Kennedy says a high-fidelity, or high-accuracy, signal cannot only reduce false alerts, but also often tell whether an employee was being malicious, negligent or whether they have been compromised. In the case of the two bank employee case studies, the Dtex platform uncovered the abnormal behaviour and showed that it was malicious.

In another recent fraud case, involving a non-Dtex customer, the company was not able to prove malice and this has been driving demand for more sophisticated systems that can help prove it, says Mr Kennedy. This is because such proof can be pivotal in achieving a prosecution. In this case, a lawyer was working on behalf of a bank in an acquisition deal. Her husband obtained non-public information from her and used it for insider trading. He had clearly acted maliciously and was prosecuted.

But there was not enough data to show whether his wife's behaviour in the incident was malicious, negligent, compromised or innocent. A more sophisticated system might have been able to prove this by providing a more detailed analysis of her behaviour.

Mr Kennedy says other legal firms have since purchased Dtex because this case highlighted the need for more evidence in such circumstances.

"They want an audit trail, so they would have a better chance of understanding what had happened in a situation like this," he says. "It would put them in the best position to either exonerate or prosecute an employee in a similar situation.

"A forensically sound audit trail makes it possible to differentiate between malicious, compromised or negligent behaviour. Without the audit trail, it is easy for staff to claim negligence or [that they were unwittingly compromised]."

As more such cases come to light and the battle against insider fraud continues to intensify, the need for intelligent technology to counter it looks set to keep growing.

100%

user threat assessments found some form of insider threat

60%

of assessments found the user utilising anonymous or private browsing to bypass security or researching how to bypass security measures

20%

of assessments found an unauthorised user of high-risk applications including hacking tools

Dtex 2018 Insider Threat Intelligence Report

For more information please visit www2.dtexsystems.com/info

OPEN BANKING

Banks cannot open up to criminals


Robin Worrall/Unsplash

New rules designed to open up banking and provide a better deal for customers require increased vigilance against possible fraud

CHARLES ORTON-JONES

A new era in banking is upon us. In January, open banking was launched across the European Union, giving a new generation of service providers a chance to thrive.

At the heart of the movement is data-sharing. Open banking, under the EU Revised Payment Services Directive, or PSD2, means third parties can link up to a consumer's high street bank account, so long as he or she consents. Mobile app Yolt is a great example. It gathers data from a consumer's multiple accounts and provides an aggregated overview of their spending habits.

But open banking might also mean a new era of fraud. RBS chairman Howard Davies warns: "We are not confident that our customers' data will be protected from hackers and thieves. We cannot refuse to hand over data because that's what the legislation says, but we will have to try to educate people to understand the vulnerability."

So what are the new threats? "Copycat websites could pretend to be third-party providers," says Chris Moses, operations manager of Blackstone Consulting, a private security agency. "Or a scammer could hack into a third party to gain access to information held in current account statements. Or pose as a third party in correspondence to extort information. This could then allow them to fraudulently access customers' money. Information, such as who your utility contract is with, could be used to extract money as part of a more complex scam."

And it might not always be hackers misusing data. Legitimate third-party providers may be the ones with a lackadaisical view on how consumer data can be used. Alex Bray, assistant vice president of consumer banking at Genpact, a technology and consulting company, sees an obvious potential abuse.

He says: "Customer data could be used for purposes other than those agreed by the customer; for example, their data could be sold on to unscrupulous marketers or fraudsters for use in identity theft." This can cause a ripple of future problems. "Fraudsters could phish for client details tricking customers into giving approval to access account information. This data could then be used to dupe customers into providing more sensitive data later."

Mr Bray stresses that startsups could be especially vulnerable. After all, high street banks have spent billions building up their digital infrastructure. Startups may be learning as they go.

The good news is that hackers will struggle to find a way through the "front door", so to speak. Open banking is built on a trusted architecture called an API (application programming interface). But there is an inferior method called screen-scraping still in use, in which the third party essentially imitates a user and goes via the consumer login. This means they need to know the consumer password in full and be able to use it in an unencrypted form.

Frans Labuschagne, head of UK and Ireland at Entersekt, a security company, says: "Screen-scraping will eventually be banned, under regulations taking effective from September 2019. But, until then, some third-party apps and websites may still rely on this method of accessing your data. Banks can't block screen-scraping; however, they could refuse to refund fraud losses if you choose to share login details with a firm that isn't authorised and regulated by the Financial Conduct Authority or another European regulator."

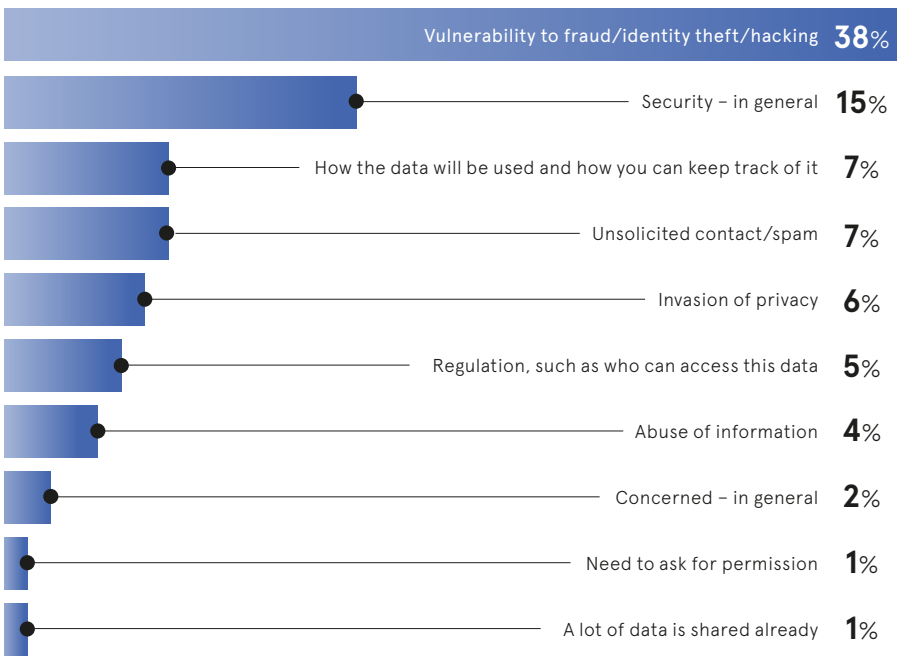
Naturally, only the very technically minded consumer will know which apps use screen-scraping. The rest of us will go in blind.

With all this in mind it is reassuring to see high street banks investing huge sums in identifying anomalous behaviour. Real-time analytics, for example, is at the forefront of risk reduction. Kai Grunwitz, Europe, Middle East and Africa senior vice president at NTT Security, says: "Banks need to mitigate new fraud risks by implementing controls based on advanced analytics to detect fraud attacks. Real-time risk analysis must detect abnormal behaviour in requests originating from third-party providers, identify suspicious transactions and, most importantly, detect atypical API calls."

The proliferation of third-party apps that can link up to a customer's bank account presents a new challenge for data security and new opportunities for fraudsters

This proactive approach can include dynamic biometrics in which consumer voice, typing and mouse movements are analysed for irregular patterns. John Erik Setsaas, identity architect at Signicat, a provider of digital identity services, says: "With dynamic biometrics, the bank can monitor usage patterns and raise flags if deviations occur. We've been speaking to several banks about how digital identity will make it simpler to grant and revoke access to a customer's account, and reduce the risk of access being in any way porous." ◆

Consumer opinion on open banking and data-sharing PwC 2018



OPINION COLUMN

‘Fraud has now become the crime of choice for terrorists’

In his evidence before the Treasury select committee of MPs, Donald Toon from the National Crime Agency, said: “It would be realistic to say that hundreds of billions are laundered through the UK annually.”

To address the threat posed by financial crime, successive governments have introduced a plethora of legislative provisions to tackle money laundering, bribery, market manipulation, fraud and the financing of terrorism.

These have achieved some levels of success and indeed the recent *Future Financial Crime Risks* report from LexisNexis Risk Solutions found that 76 per cent of compliance professionals expected legislation to decrease money laundering in the UK. Terrorism financing, however, is not only very difficult, if not impossible, to prevent, it is also a subject that no one wants to discuss.

The European Union is suffering from the second decade of the most intense wave of international terrorism since the 1970s, when countries have been subjected to an increasing amount of low-cost terrorist attacks.

These attacks have three common themes: evidence of a sophisticated terrorist support network; the use of low capability weapons; and inexpensive acts of terrorism.

For example, recent acts in Barcelona, London, Paris and Stockholm have involved terrorists using a rental vehicle to target pedestrians. Of course, the relative ease of self-funding this vehicle rental provides further evidence to demonstrate how inexpensive forms of terrorism can exploit loopholes in counter-terrorist financing legislation.

Preventing terror financing is extremely difficult because of the large number of funding mechanisms. Traditionally, terrorists relied on two sources of funding: state and private sponsors.

Since the terrorist attacks in 2001, state-sponsored acts of terrorism have declined and terrorists have generated funds through a broad spectrum of illegal mechanisms, including kidnap for ransom, armed robberies, drug trafficking, counterfeiting and the sale of conflict diamonds.

However, fraud has now become the crime of choice for terrorists who have acquired funding via benefit and credit card fraud, identity theft and the sale of counterfeit goods.

The association between terrorism financing and fraud was first associated with the IRA, who accrued its funding via tax fraud. The Financial Action Task Force has also noted that al-Qaeda often receives funding via credit card fraud.

In the UK, the connection between terrorism and fraud is illustrated by the conviction of Yahya Rashid, who spent his student loan and other grants on travelling to join Islamic State, and it has been suggested that suicide bomber Salman Abedi used taxpayer student loans to fund the Manchester Arena attack.

Charities are also susceptible to abuse by terrorists who are seeking to accrue finances via the exploitation of charitable payments. Following 9/11, it was estimated that approximately 30 per cent of al-Qaeda finances were obtained from misapplied charitable donations and, as a result, the US Treasury Department blocked the finances of 40 charities, including the Holy Land Foundation in Texas.

Terrorists will seek to use associated charities because it provides an element of authenticity for the transfer of funding, a technique that has been frequently used by Boko Haram across Africa too.

Closer to home, the Home Office identified the link between terrorism financing and charities in 2017 when is reported that charitable donations worth hundreds of thousands of pounds were unwittingly sent to Islamic extremists. Interestingly, the Home Office refused to publish the full report, thus limiting understanding of this funding stream.

The threat posed by terrorism and its financing is unprecedented, and there are clear gaps within the existing counter-terrorism financing legislative frameworks that require a radical rethink.

Unless these legislative deficiencies are tackled, terrorists will continue to attract funds via an unprecedented array of illegal mechanisms. It is essential that law enforcement agencies and the Charities Commission work together to limit this attractive and common funding stream for terrorists.

Dr Nicholas Ryder
Professor of financial crime
University of the West of England

Commercial feature

Convergence of fraud and compliance in fight against financial crime

To build better customer relationships and increase profits, enterprises must converge their fraud and compliance solutions, and remove the silos that allow sophisticated criminals to take advantage

Matt Cox
Senior director of fraud, cyber and compliance, EMEA, FICO

The fraud industry has evolved in the last ten years from focusing almost entirely on simply stopping fraud and the subsequent losses, to balancing those objectives with maintaining a strong customer experience and complying with regulatory change.

Simultaneously, criminals have evolved and become more sophisticated. Those fighting financial crime may see money laundering and fraud as the business of different departments, but criminals see no such barriers. Money obtained through fraud, or other criminal activity, is laundered through accounts almost seamlessly.

In today’s world of real-time payments, hopping the proceeds of crime through multiple accounts and out of the system helps criminals to gain control of their ill-gotten gains, and foils the attempts of law enforcement to trace and stop them.

Taking a more holistic approach to fighting financial crime is challenging. Many organisations, particularly those that have grown through acquisition, struggle with a legacy of multiple-point solutions that are embedded into core business systems. This results in silos and a lack of visibility across the financial crime life cycle; criminals take advantage of this.

A typical enterprise has both fraud and compliance departments. The fraud team is primarily responsible for fraud losses, while the compliance team helps the organisation to stay on the right side of financial crime legislation, most notably the regulations that govern money laundering and tax evasion.

The departments require much of the same information and both must take appropriate action when financial crime is suspected, but if they don’t share information then neither has a full picture of the customer. Numerous systems are maintained, which means maintaining multiple teams with their own skillsets that are not transferrable.

2.6bn
payment cards protected worldwide by FICO’s fraud management system

0.5bn
transactions a day screened by FICO technology for money laundering and other financial crimes

Customers can become frustrated with the inconsistency, such as having to provide the same information twice, and cases are often progressed inadequately when information is not available when needed. Running in silos makes the departments more costly to run, increases losses and prevents less financial crime, all impacting the bottom line.

“The fraud and compliance functions need to come together and take a holistic approach to the people, processes and solutions they use,” says Matt Cox, senior director of fraud, cyber and compliance, Europe, Middle East and Africa (EMEA), at FICO. “Then when the customer opens an account, or spends or moves money, the bank can check for money laundering and potential fraud at the same time.

“If something suspicious happens, the customer doesn’t want two different phone calls from the fraud and compliance teams. Too often that happens these days, so convergence is a must.”

FICO is leading the enterprise management approach to financial crime by helping their clients tackle both fraud and compliance. The analytics software firm, which has the world’s leading payments fraud management system, identified the issues silos were creating several years ago and in 2016 it acquired TONBELLER, which has a large footprint in the compliance space.

“Forward-looking organisations are considering how they bring people, processes and technology together,” says Mr Cox. “Over half of our clients consider a converged financial crime operating model to be their next logical step. Convergence allows enterprises to protect all channels, protect their customers, create a consistent customer experience and maximise loss prevention and revenue. At the same time, institutions can remain compliant and can take more responsibility for financial crime across the life cycle.”

FICO’s approach to tackling all aspect of financial crime builds on its significant history of using artificial intelligence and machine-learning. FICO uses multiple, patented machine-learning techniques to look for behavioural anomalies that could indicate either fraud or money laundering.

“We were the first to bring machine-learning to fraud in the US and then took it around the world,” says Mr Cox. “Now we’re applying the technology to beat more types of financial crime.”

For more information please visit FICO.com/fraud

FICO®

ILLEGAL INSIDERS

According to the latest research, occupational or internal fraud is more often than not perpetrated by a man in a position of authority who is out for personal gain through the deliberate misuse of a company's resources or assets. Exploring the data associated with this type of crime can help organisations understand the patterns to look out for and the common characteristics of a typical offender

52%

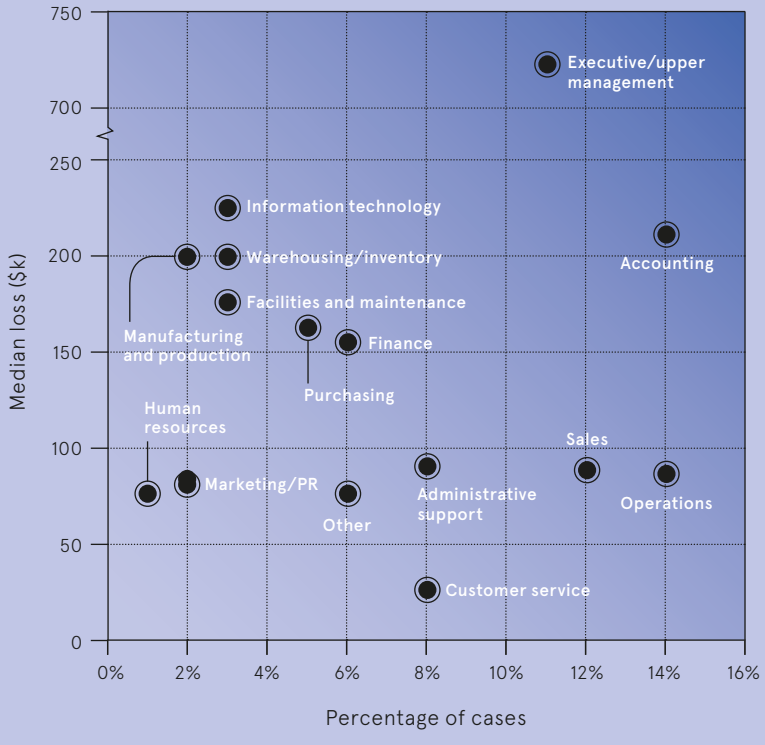
of all reported frauds over the past 24 months were cases of internal fraud, up from 46 per cent in 2016

$90k

average loss for organisations as a result of occupational fraud

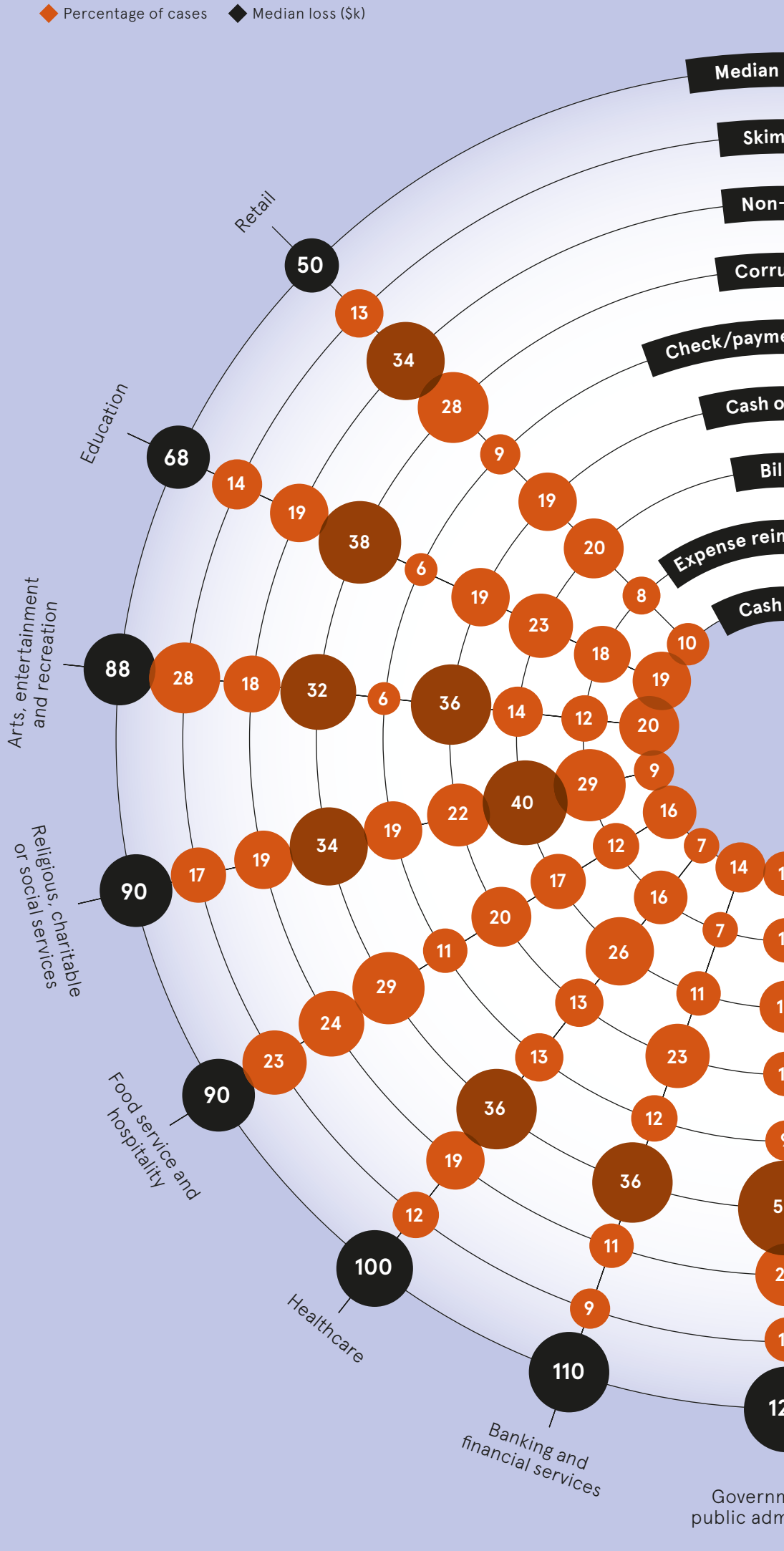
Global Economic Crime and Fraud Survey 2018, PwC

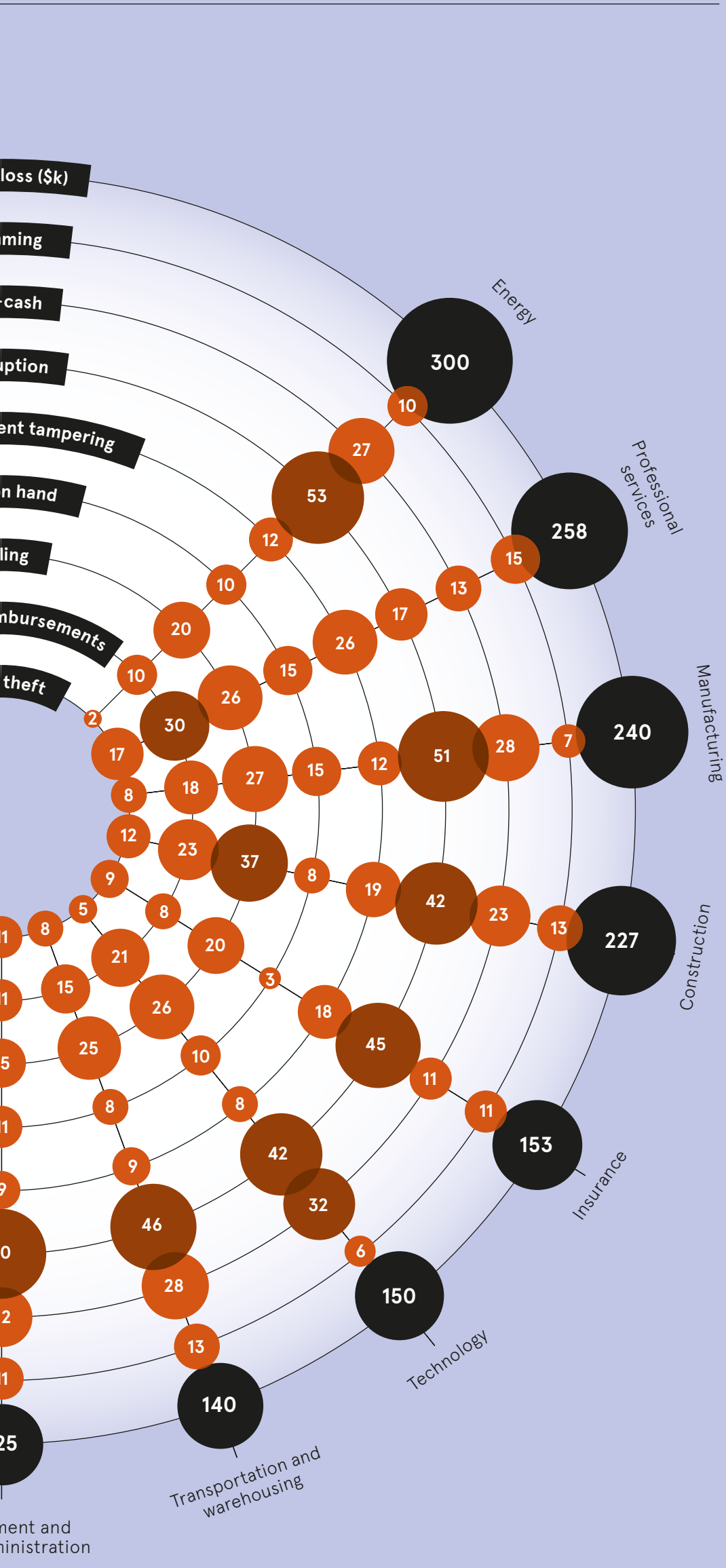
Departments that pose the greatest risk for occupational fraud



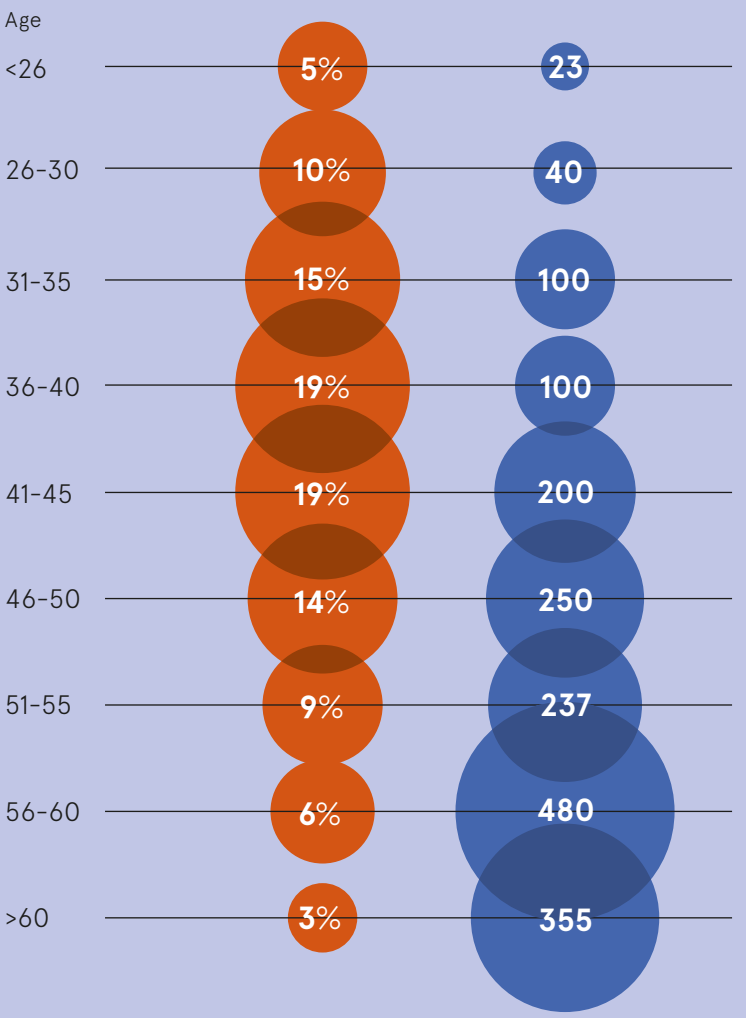
Most common occupational fraud schemes by industry

Based on more than 2,000 cases of occupational fraud worldwide; least common frauds such as financial statement fraud, payroll fraud and register disbursements have been omitted

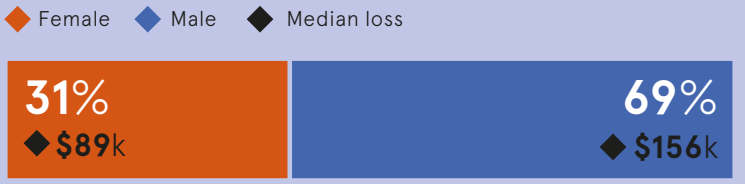




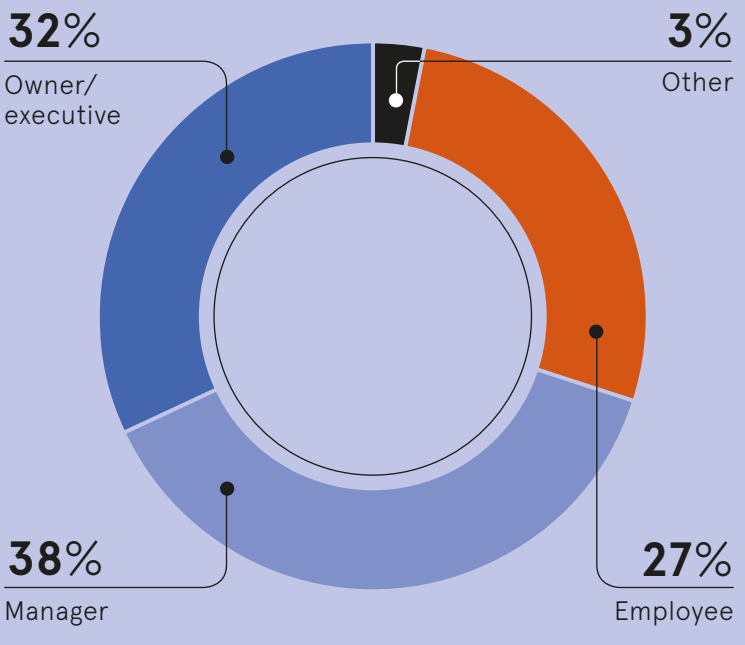
Occupational fraudsters by age



Occupational fraudsters by gender



Occupational fraudsters by seniority



***2018 Report to the Nations*, Association of Certified Fraud Examiners**
Based on more than 2,000 cases of occupational fraud worldwide

Commercial feature

Q&A Digital platforms bring fraudsters together to threaten business

Tim Ayling, global head of Fraud Prevention Solutions at Kaspersky Lab, calls for businesses to remember the crucial 'information' element in information technology as the evolution of fraud threatens them both financially and reputationally in the digital age

How has the digital threat landscape evolved in recent years?

A key change that we've seen in the digital space is the way the fraudsters have come together to form a community. Undoubtedly the dark web has played a huge role in this, but it is now commonplace to see information being shared on open social networks to help each other succeed in perpetrating fraud. There's also a big market for tools that can launch malware, phishing scams and more. This has made it much easier for fraudsters to launch fraud attacks as the hard work is done. There's now even a growing market for "fraud-as-a-service" where you can ask for a certain organisation to be targeted and they will do it for you. These are highly professional outfits that offer 24-hour support, a choice of payment options and will interact openly with you on social media.

In what ways is fraud typically carried out in the digital world?

We could talk all day about the different types of fraud in the digital world. The Nigerian Prince scam is still the most common, though in different guises and now not just via email, but also Facebook, LinkedIn, instant messaging and more. Phishing is still prevalent, where malware links are sent to people via email, though SMishing is also popular where email is replaced by SMS. Moreover, besides new and traditional kinds of malware, other means are used either to get access to a legitimate account or to steal login credentials. Social engineering is still popular, while the use of automated tools, such as bots or remote access software, are on the rise. While organisations across all verticals will have fraud prevention measures in place to fight this, fraudsters offer training and knowledge-sharing to help find a way past well-known fraud management solutions.

Tim Ayling
Global head of Fraud Prevention Solutions, Kaspersky Lab

What are the financial and reputational consequences of suffering digital fraud?

That's a very timely question, with the European Union's GDPR (General Data Protection Regulation) having come into effect in May. If breached, businesses can now be fined either €20 million or 4 per cent of global turnover, whichever is greater. That's a massive incentive for organisations to do the right thing when it comes to protecting their customers' personal information. Of course, fraud can occur without a data breach, so GDPR isn't the be all and end all of it, but it helps bring these issues to board level as there's an immediate potential of a crippling fine. Before GDPR, the bigger problem was brand damage. What we've learnt is that much depends on the response to these attacks and any fraud-related issues. People tend to be forgiving of organisations that are open about a breach, but punish those that are more secretive.

How does Kaspersky Fraud Prevention help companies protect their business and customers?

Kaspersky's success is built on the threat intelligence information we have gathered during more than 21 years in the security industry. In 2017 alone, we discovered an average of 3.25 million online attacks a day. This is unprecedented in the fraud prevention industry and hugely important. Over the past 20 to 30 years, organisations of all sizes have spent billions, if not trillions, of pounds on technology. While this has certainly brought efficiencies, it has not really provided competitive advantage. Businesses are now waking up to the importance of the information piece of IT. Technology without information is limited and flawed. In the finance sector, for example, we identified 294 fraudulent accounts in four different banks connected to Kaspersky Fraud Prevention Cloud and uncovered a massive cross-banking money laundering group. In retail, we identified and blocked a fraudulent scheme involving 3,000 accounts in a network loyalty programme. Kaspersky Fraud Prevention will continue to use that information for good, and supplement it with new information and technology through behavioural analytics, biometrics, machine-learning and device analysis.

3.25m
online attacks a day discovered in 2017 alone

294
accounts from a fraudster ring identified in four different banks

3,000
fake accounts identified and blocked in a retail loyalty programme

For more information please visit kaspersky.co.uk/enterprise-security/fraud-prevention

KASPERSKY lab

Fraud now threatens the way we live

Fraud, like the mythical Hydra of Ancient Greece, is a many-headed foe that is capable of disrupting society in a number of ways

OLIVER GRIFFIN

Fraud has existed since time immemorial. The first recorded instance was in 300BC, committed by an incompetent Greek seafaring merchant called Hegestratos. He planned to defraud an insurer by sinking his ship, empty of cargo, and selling the corn supposed to be on board. Unfortunately for Hegestratos, his scheme was discovered and he drowned after escaping his passengers, no doubt angry at his plan to kill them.

Fast forward to the 21st century and the capabilities of fraudsters have reached new heights, to the point where they now pose the risk of destabilising global economies and governments.

In 2016, Colombian hacker Andrés Sepúlveda confessed to rigging elections across Latin America during an eight-year period. Since then, the UK's Brexit vote and the United States' election of Donald Trump as president have come under scrutiny as investigations probe whether or not hackers influenced voters with fake news.

"The fraud schemes we see are always changing, as the ways in which people interact with each other change," says Fran Marwood, investigations partner in the forensic services team at big-four accounting firm PwC.

"Fraud has evolved massively over the 20 years I've been investigating it. The two biggest factors have been the increase in global communications, and the huge developments we've seen in technology and the use of data. Smartphones are only just over ten years old, which puts the changes into perspective."

Financial crime and other fraud has the capacity to destabilise global economies through its ability to steal increasingly large sums of money and change the path of history as fraudsters manipulate events for their own means.

But while the impact of electoral fraud has demonstrated its power to threaten economies' growth, financial fraud still continues to rear its head. In January it emerged that a middle manager and a subordinate in India's Punjab National Bank had quietly executed a fraud since 2011, stealing some $1.8 billion.

"The fraud didn't go down well with the regulators, with the political machinery and of course with the general public," says Tarun Bhatia, managing director and head of South Asia in Kroll's investigations and disputes practice. "It happened in a sector which has seen similar issues, so there was also concern around lack of learning and processes in place."

A PwC report published earlier this year found that more businesses had experienced fraud in 2017 than in 2016, increasing to 49 per cent of respondents from 36 per cent previously. The firm's *Global Economic Crime and Fraud Survey* also found that cybercrime is predicted to be the most disruptive fraud facing organisations over the next two years.

As problematic as they are, financial crimes are far from the most sinister plans that fraudsters could hack to destabilise global economies. Campaigns of misinformation can also trick populations into letting their guard down, with potentially devastating results.

A recent study by the *American Journal of Public Health* found that online trolls from Russia posted tweets for and against vaccination, with the aim of sowing discord among the US population. "Accounts masquerading as legitimate users create false equivalency, eroding public consensus on vaccination," the report says, explaining that the trolls were attempting to bring further division to US society, as well as eroding public faith in important vaccines.

A sudden drop in vaccine use could significantly destabilise global economies and the US might be the first victim. Illness costs countries billions every year, but a serious pandemic, caused by a rise in infectious diseases due to less people vaccinating their children, could decimate economies. The Spanish flu, which lasted from 1918 to 1920, is thought to have killed 100 million people and wiped around $4 trillion from global GDP, around 5 per cent of the total.

Fraudsters sowing discord to stop countries from fulfilling important


Denys Nevozhai/Unsplash

vaccination programmes could have a similarly devastating impact. The World Bank forecasts that a global pandemic would have an equally disastrous effect on the 21st-century world economy.

The threat posed by fraud to destabilise global economies should not be underestimated. Criminals get more organised and pose different challenges to those who are trying to thwart them.

"It's starting to get more and more sophisticated to stop fraudsters attacking," says Nick Mothershaw, director of fraud and identity solutions at Experian. "They'll up the ante and we'll get better at defending. It's a guerrilla warfare; it continues to be so, but we are getting better at it."

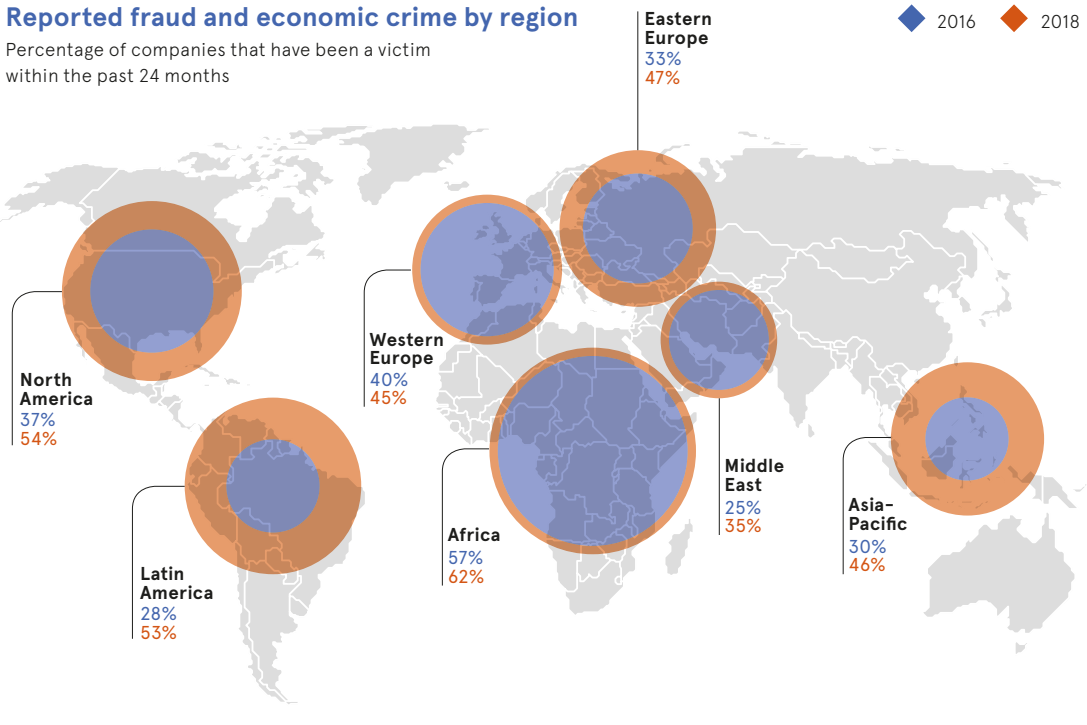
> **Those tasked with fighting fraud and preventing the destabilisation of global economies have to stay one step ahead**

The fact is that the fight against fraud is an ever-evolving arms race. The threat fraudsters pose to businesses, governments and other organisations means those tasked with fighting fraud and preventing the destabilisation of global economies have to stay one step ahead.

"The biggest factor here is technology, and the opportunities that it presents fraudsters to steal cash and other assets," Mr Marwood says. "I have no doubt that these opportunities will increase and develop over time. Technology has two sides though, and can be highly effective in preventing and detecting fraud. The worst-case scenario is that government, businesses and individuals don't keep up with the fraudsters." ◆

Reported fraud and economic crime by region

Percentage of companies that have been a victim within the past 24 months



While prevalence is higher in certain regions, this is only the reported rate, where companies are actually aware they have been victims of fraud and economic crime

PwC 2018

MARKETING

Growing call for action against fakes

Marketing fraud, ranging from fake news disseminated by robots, to fraudsters syphoning off advertising cash, is coming under increasing scrutiny

GIDEON SPANIER

When the world's biggest advertiser warned the digital media supply chain is "murky at best, fraudulent at worst", it rang alarm bells in boardrooms and marketing departments around the globe.

Marc Pritchard, chief brand officer of Procter & Gamble, made the comments in a landmark speech to the US internet industry in January 2017 and, nearly two years later, fears about marketing fraud have only increased, even if awareness of the problem has also risen.

It should be in the interests of all the players in the media supply chain – advertisers, their agencies and other intermediaries, internet platforms and publishers, regulators and law enforcement – to clean up the digital ecosystem.

But it is hard to keep up with criminals who exploit the global nature of the internet and are always seeking to stay one step ahead of the law, particularly as technology continues to evolve rapidly and constant vigilance is required.

Juniper Research has warned that marketing fraud will cost advertisers an estimated $19 billion (£15 billion) and rising in 2018, close to 10 per cent of global digital ad expenditure.

The research firm identified the main problems as fake websites and internet domains, fake accounts, and bot farms that generate fake views by robots, not people.

Mobile is the new battleground. Ad fraud on mobile devices has jumped eight-fold in the last year as smartphone use has increased and desktop fraud has come under greater control, according to Double Verify, a company that helps advertisers to check their media and marketing spending.

Mobile app "spoofing" and "hidden" ads that are "fraudulently diverting brand investments" are among the problems cited in DoubleVerify's *2018 Global Insights Report*.

> **The main problems are fake websites and internet domains, fake accounts, and bot farms that generate fake views by robots, not people**

The measurement company also warns that brand safety "violations", where ads appear next to inappropriate content, have risen 25 per cent this year because of a "surge in fake news and unsubstantiated content".

Marketing fraud has also become a political issue, after evidence emerged that bad actors from outside the United States tried to influence the outcome of the 2016 US presidential election by micro-targeting audiences with messages, some of which contained dubious and fake claims.

Other areas of the media supply chain have come under scrutiny, even though some players may be guilty of "murky", rather than "fraudulent", behaviour.

Automated ad-buying, known as programmatic trading, has raised concerns because there are lots of intermediaries that may be taking a cut in the supply chain, as the money passes through advertising exchanges, which aggregate buyers and sellers of ad inventory. Some advertisers have found that when they spend £1 on digital media as little as 30p is reaching the publisher.

Brands have also raised questions about affiliate marketing, where third parties receive a cut for driving ecommerce sales, and influencer marketing, where brands pay social media influencers to endorse products.

MPs on the Commons Digital, Culture, Media and Sport (DCMS) select committee have suggested the Competition and Markets Authority (CMA) could investigate fake accounts to see if advertisers are being charged for reaching an audience that doesn't exist.

Advertisers have faced similar problems with viewability, being charged for ads that can't be viewed properly or are viewed by bots.

The digital media ecosystem does indeed look murky. However, Martin Vinter, head of media at Ebiquity, a UK-based consulting and media auditing firm that advises hundreds of global advertisers on their marketing spending, says it may not be helpful to lump all these different areas together under the catch-all phrase "marketing fraud" or "advertising fraud".

"It's an umbrella term for many different things," Mr Vinter says. "We've slightly skewed the conversation to fraud."

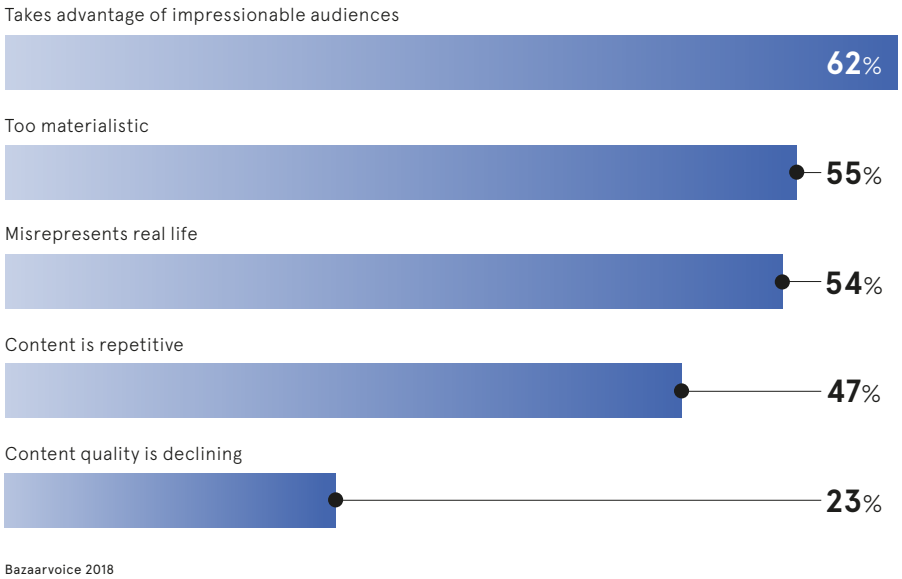
He believes it's important to distinguish between fraudulent and criminal behaviour, such as website or app spoofing at one end of the spectrum, and lax or poorly defined standards around viewability at the other end.

The ad industry has functioned for many years through a system of self-regulation and the law is notoriously slow to catch up with technology. So advertisers may still be best placed to take responsibility for cleaning up what Keith Weed, chief marketing and communications officer of Unilever, the world's second biggest advertiser, calls the "digital swamp".

01 Not knowing whether you've been pitched to via influencers on social media is a growing issue

02 Marc Pritchard, chief brand officer of Procter & Gamble, says the digital media supply chain is "murky at best, fraudulent at worst"

Consumer opinion about influencer content



Bazaarvoice 2018

92%

of consumers interact with influencers on social media

Bazaarvoice

50%+

of engagement with a single day of Instagram posts tagged #sponsored or #ad were found to be fake

15%

of influencers who sign on to do sponsored posts in return for a product never create a post

Sway Ops

Mr Vinter believes advertisers have been making progress in tackling the supply chain. "Affiliate marketing used to be a Wild West until people started to take control," he says, explaining how third-party verification of online activity has brought independent accountability in recent years.

Similarly, programmatic trading has begun to clean up its act after intense scrutiny.

Advertisers have been tightening up their contracts with agencies, demanding that intermediaries disclose how much each of them might be taking as a cut or getting as a rebate, and doing direct deals with the big tech platforms such as Google and Facebook.

Publishers have also introduced ads.txt software that identifies authorised buyers and sellers on advertising exchanges to combat the problem of domain spoofing and fake clicks.

"Unauthorised" buyers who act as intermediaries on behalf of advertisers and charge for ads that never appear are a serious problem.

The Guardian and Google carried out a joint test on the newspaper publisher's inventory this summer when they bought display and video ads without using ads.txt. They discovered that some unauthorised ad exchanges were charging for ads on *The Guardian* yet no ad appeared and no money reached *The Guardian*.

An astonishing 72 per cent of video ad spend that *The Guardian* bought in its test without ads.txt was going to unauthorised exchanges.

Mr Vinter says advertisers and publishers are waking up to the need for more third-party checks and verification to monitor marketing investments. "Verification is the panacea," he believes.

Influencer marketing is another minefield in need of tougher standards. Unilever's Mr Weed told the ad industry's annual festival, Cannes Lions, in June that urgent action is required to tackle problems such as influencers "buying" followers.

Facebook and Twitter have both come under pressure to shut down fake accounts. At one stage, Twitter was suspending as many as one million accounts a day earlier this year.

"Influencer marketing is probably now in the place where affiliate marketing was," Mr Vinter warns, adding that lack of verification standards could potentially pose more harm to a brand's safety because of the reputational risks of partnering with a dishonest influencer.

The awkward truth for brands is that the digital ecosystem is complex and fragmented, and they can't tackle marketing fraud in isolation.

As Wayne Gattinella, chief executive of DoubleVerify, says: "It's critical that digital marketers around the world have a holistic approach to brand safety, digital ad fraud and viewability."

There are signs that regulators and politicians are helping to apply pressure.

Sharon White, chief executive of Ofcom, the UK's communications regulator, believes "the argument for independent regulatory oversight" of tech companies "has never been stronger" when it comes to fake news and disinformation.

> **The awkward truth for brands is that the digital ecosystem is complex and fragmented, and they can't tackle marketing fraud in isolation**

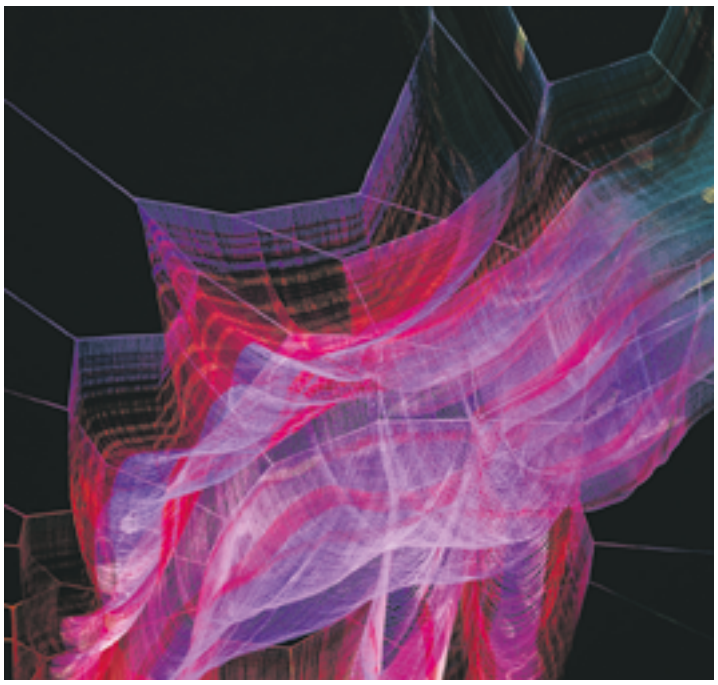
The Commons DCMS select committee has already published a report that was scathing about Facebook and Cambridge Analytica's misuse of data, and is planning a follow-up study of flaws in digital advertising.

The unanswered question is whether the CMA in the UK, the US Department of Justice or another law enforcement body will launch a legal investigation into marketing fraud.

But the immediate responsibility should rest with advertisers because it is their money. They have the greatest power to demand change from agencies, publishers and internet platforms by refusing to spend with anyone unless they are accountable and transparent. ◆

Complex fraud threats call for adaptive detection tools

Collating varied types of data in different formats and making sense of them by applying machine-learning will enable businesses to counter security threats



The payments and ecommerce landscape has undergone significant changes in recent years. At a local level, commerce and banking moved to a digital-first, standard format. At a global level, and specifically in developing markets, there has been a huge transition from "mum and dad" shops straight to online commerce. People no longer need banks or shops; they need banking and commerce services.

However, as much as this offers new and exciting online opportunities to business, unscrupulous individuals are also taking advantage of easy-to-access fraud tools, exploiting vulnerabilities and targeting weaknesses in the security infrastructure of unsuspecting organisations.

Rahul Pangam, co-founder and chief executive of fraud prevention technology firm Simility, acquired by PayPal earlier this year, believes that companies are now operating in an environment where they have to assume, even with the most sophisticated security solutions, there are no cast-iron guarantees in a "post-breach normal" world.

"How to manage risk in this environment is different than how to manage it in a world where data can't be compromised. As transactions happen, risks need to be managed in real time," says Mr Pangam.

The most pressing challenge for companies is to balance customer experience effectively with security and regulatory issues. Customers have become accustomed to frictionless digital experiences and want payments to be made immediately, at the same time as cybercriminals are utilising increasingly sophisticated techniques. An increasingly complex regulatory environment that necessitates businesses comply with PSD2 (Second Payment Services Directive), faster payments and open banking adds a further burden to firms.

Rahul Pangam
Co-founder and chief executive Simility

"It's not realistic to treat every user as a fraudster, as they will dislike the experience and go to a competitor, but equally trusting each login attempt will let fraudsters in at some point," says Mr Pangam. "Achieving the best of both worlds by offering a positive user experience and implementing appropriate fraud prevention solutions can be achieved by analysing each user and their activity in a nuanced way."

Fraud management is no longer a linear decision, with multiple factors needing to be considered and weighted in real time, which is something traditional tools are unable to accomplish. By focusing on a single instance of fraud or cybercrime, the wider context is ignored. For example, fraudsters may move money from a savings account to a current account and leave the money untouched. The bank may find this suspicious, but they might not act on it, then a fraudster may use a stolen ATM card to cash out the account.

"Two distinct events may not seem related on the surface, but by using platforms such as Simility to harness disparate data, actionable insights can be uncovered to identify anomalies," says Mr Pangam.

Data is the driving force behind effective fraud management and businesses that are able to turn data into a strategic advantage will have an edge over competitors. Simility's Adaptive Decisioning Platform was built with a data-first approach in mind and offers a complete view of customer behaviour and activity, which ensures every piece of information can be utilised and all regulatory requirements are met.

The multi-channel aspect of fraud is increasing as fraudsters are becoming even more adept at circumventing security tools. Pulling together varied types of data in different formats and making sense of them by applying concepts of machine-learning will enable businesses to adapt effectively to future security challenges.

With Simility, businesses not only have the processing power to analyse huge datasets, but they also gain the ability to customise user interactions. "If you see access from a new location or device, while it could be the user travelling, it could also be a fraudster. Why ask all users the same verification questions? Personalise services based on risk factors, such as location, device and behaviour, to make the process more seamless," Mr Pangam concludes.

For more information please visit simility.com

simility
A PayPal Service

This technology can help

Hailed as a tamper-proof public ledger, blockchain is a welcome weapon in the fight against fraud

DAVID COWAN

When new technological solutions emerge they are often hailed as a panacea for all things, including fraud. Can blockchain prevent fraud as a silver bullet? No. But it's a welcome addition to the arsenal of fraud prevention and a significant step towards squeezing out the fraudsters.

Eric Wall, cryptocurrency blockchain lead at technology company Cinnober, is dismissive of the hype. He says: "Everyone with blockchain knowledge agrees that in reality blockchains are specific solutions for a specific problem. The idea it's a silver bullet is spread in the media and by people new to the technology."

Because blockchain is a decentralised shared ledger and resistant to tampering, it certainly offers some robustness to transactions. Verified users can store, view and share digital information in a security-rich environment. This helps to foster trust, accountability and transparency in transactions, all important aspects of commercial relationships, and can be applied to financial transactions, identity management and the supply chain.

It is used in maintaining asset registers for shares, property, smart contracts, and other titles to ownership and documentation, all making such fraud more difficult. However, it should not be forgotten that technology is equally an enabler of fraud.

According to the *2017 Identity Fraud Study* by Javelin Strategy & Research, identity theft and fraud is costing consumers $16 billion a year and 15.4 million people were victims. American Express is investigating ways in which blockchain can be used to safeguard user identities, as well as helping merchants securely process transactions.

Tereasa Kastel, American Express vice president technology, says the company is examining several avenues for blockchain. She says: "Being in the financial industry, we have to be somewhat conservative on what legal and regulatory

Insight

Point of entry

The UK's National Fraud Intelligence Bureau (NFIB) defines fraud as happening "when trickery is used to gain a dishonest advantage, which is often financial, over another person".

There are numerous forms of fraud, the most prevalent being Ponzi-schemes, pyramid schemes, identity fraud, mortgage and lending fraud, phishing, card fraud, skimming, counterfeit cards, advance fee scams, fund transfer scams, fake prizes, inheritance scams, false wills and legacies, and international lottery fraud. The more we digitise, the more we can record, track and detect patterns in such frauds.

What these frauds have in common is behaviour. The NFIB notes there are many words used to describe fraud: scam, con, swindle, extortion, sham, double-cross, hoax, cheat, ploy, ruse, hoodwink, confidence trick. These have been around since the beginning of the human race, as they are all behaviours rather than the specific means of perpetrating fraud.

Technology has enhanced the means and made fraud more global, but the key focus becomes the point of entry. If employees do not protect passwords or individuals give out identify information, then the fraudsters can use these as points of entry. Technology then simply automates the folly.

Blockchain's appeal is that all transactions take place on a public ledger; no individual or group of individuals can tamper with financial data and there is complete transparency. According to the *Certified Public Accountant Journal*: "Blockchain can effectively prevent one or several individuals in collusion from overriding controls, or illicitly changing or deleting official accounting records." However, this doesn't address the point of entry problem or bad data at origin. Blockchain is part of an anti-fraud ecosystem, which includes various new technologies such as biometrics, tougher regulatory regimes for customer identification, such as know-your-customer rules, anti-money laundering regulations and data protection laws, aimed at defending fraudsters' potential point of entry.

bricksters to book

requirements there are, but on the other hand, what I would say is that what it empowers an individual user to do in terms of controlling their identity, and have that identity be immutable, is something you can't pass by, despite what might be the regulatory controls at this time."

Specific industries and services are particularly vulnerable to fraud. The National Health Care Anti-Fraud Association conservatively estimates healthcare fraud to cost the United States about $68 billion annually, representing 3 per cent of total $2.26 trillion US healthcare spending.

On the global stage, foreign aid is rife with corruption, and funds intended to help people on the ground finds its way into the hands of corrupt officials and militia groups. John J. Sullivan, US deputy secretary of state, addressing last year's Blockchain Forum in Washington, explained: "Two major challenges in foreign assistance that blockchain technology could address are, first, corruption, fraud or misappropriation of funds and, second, inefficiencies within the aid delivery process itself."

Don Tapscott, chief executive of the Tapscott Group and co-author of *Blockchain Revolution*, says: "That's why it's called blockchain, and that block is linked to the previous block and the previous block, ergo, chain. This blockchain is running across countless numbers of computers. I would have to commit fraud in the light of the most powerful computing resource in the world, not just for that ten-minute block, but for the entire history of commerce, on a distributed platform – this is not practically feasible."

However, we should be careful not to hype it up too much. Blockchain can increase the efficiency of transaction processing and reduce fraud, but it doesn't entirely prevent it and risk officers would be unwise to ignore its limitations.

> **I would have to commit fraud in the light of the most powerful computing resource in the world - this is not practically feasible**

Mr Wall highlights high-performance environments such as financial trading, where speed of transactions can mean the difference between massive profits and even bigger losses. Blockchain is inherently slow in the validation process. He says: "It can only see an order and process it; what it can't understand is the trading context and see if fraud is involved."

Initial coin offerings (ICOs) are another good example of limitations. Last year JPMorgan Chase chief executive Jamie Dimon attacked bitcoin claiming cryptocurrency is a fraud and a mania reminiscent of the tulip bulb craze in the 17th century. If the prospectus is based on a tissue of lies, then the ICO blockchain will simply validate the integrity of a fallacy. Mr Wall adds: "In ICOs, blockchain can become the facilitator of a fraud."

People commit fraud, not the technology, and the art of fraud is getting into and out of the system. Succeed in that and the rest is the system doing its normal job. If an employee or person with authority to act can find a way into the transaction, then it is difficult to monitor.

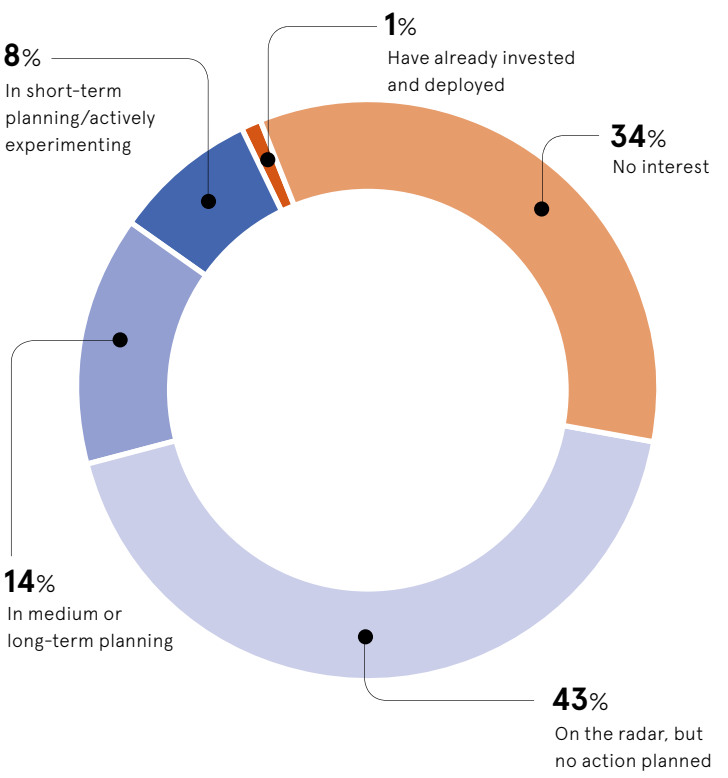
Mr Wall says: "Any information processing system that has bad input provides bad output. The blockchain can only be aware of the inputs, not the reality. The blockchain will track it as valid data, so if you have the authority to input bad data, then the blockchain will validate the bad data. You still have a dependency on the real world, trusted sources of data and authorisation. If you corrupt that then you corrupt the process."

Unlocking the full potential of blockchain technology will need governments to work as a facilitator, by providing an enabling environment to interested players. There is a need to develop uniform standards, assess infrastructure requirements, deal with security concerns, raise stakeholder awareness and build trust within the financial ecosystem as a whole. This should be done in partnership with risk managers, enforcement agencies and others tackling fraud.

However, greed, speculation and fraud are not financial mechanisms; they are behaviours and, as long as we have human behaviour, we will have fraud. ◆

Blockchain deployments still scarce

Global survey of chief information officers shows the extent of organisations' blockchain deployments



Gartner 2018

CyberSource®
A Visa Solution

Powered by machine learning. Controlled by you.

Win epic battles against fraud using smart machine learning, combined with flexible rules. CyberSource Decision Manager combines machine learning with rules that let you precisely control your online fraud management strategy.

Half human, half machine – the best of both worlds.

cybersource.co.uk/machinelearning